Office of the Attorney General
Paul G. Summers

Department of Commerce and Insurance
Commissioner Paula Flowers

NEWS RELEASE

Office of the Attorney General
P.O. Box 20207 Nashville, TN 37202-0207

Department of Commerce and Insurance
Division of Consumer Affairs
500 James Robertson Parkway Nashville, TN 37243

FOR IMMEDIATE RELEASE
Feb. 9, 2005
#05-03

CONTACT:
Sharon Curtis-Flair
(615) 741-5860

STATE ATTORNEY GENERAL ALERTS CONSUMERS TO "PHISHING" E-MAILS

"Phishing" is a high-tech e-mail scam aimed at stealing your identity, and it continues to be a problem nationwide, according to Tennessee Attorney General Paul G. Summers and Mary Clement, director of the Division of Consumer Affairs, who earlier this week kicked off National Consumer Protection Week.

"Phishers" often send e-mails purporting to be from banks or other financial institutions to consumers to trick them into disclosing information such as account information, credit card numbers, Social Security numbers and other sensitive information. One Tennessean recently received an e-mail, deceptively claiming the customer's bank was undergoing a software upgrade and needed the customer to confirm "customer data" by going to a particular link on the Internet.

"Once you surrender your personal information, it is simple for a 'phisher' to steal money from your bank account," said Attorney General Summers. "They may also use personal information to apply for a job, obtain credit or buy a house in your name."

Other versions of "phishing" include e-mails threatening to suspend consumers' access to financial accounts if they don't immediately provide or confirm personal information. Some e-mails indicate there are pending transactions in the consumer's account that require the consumer's approval. Many "phishing" e-mails contain the legitimate company's images or logos to help make

them appear authentic.

Attorney General Summers and Mary Clement offer the following suggestions to help consumers to determine if an e-mail is legitimate or "phishing" and how to handle it:

*Be wary of e-mails with a sense of urgency that contain misspelled words or grammatical errors.
*Being able to click anywhere in the e-mail and not just on the link may indicate "Phishing."
*Other indicators include writing that is stilted or awkward and poor visual or design quality.
*If you receive an e-mail you believe may be "Phishing," go to the company website by typing the company's web address into the browser or by doing an Internet search for the company rather than clicking on the link provided. It may direct you to a "spoof" website designed to look like the legitimate site.
*Check for fraud alerts posted by the company.
*Report the e-mail to the company. Instructions for making these reports can often be found on the company's website.
*If you've provided personal information in response to an e-mail you believe may have been "phishing," alert your bank and the three major credit bureaus. You can report fraud to Equifax at 1-800-525-6285, to Experian at 1-888-EXPERIAN and to TransUnion at 1-800-680-7289. You can also report the suspicious e-mail to the Federal Trade Commission at www.consumer.gov/idtheft or 1-877-IDTHEFT. Finally, contact the Tennessee Division of Consumer Affairs at (615) 741-4737 or www.state.tn.us/consumer.

Feb. 6-12 has been designated as National Consumer Protection Week with a focus on identity theft.